EDITAL DE SELEÇÃO PARA COOPERAÇÃO EM EXECUÇÃO DE POLÍTICA PÚBLICA
RNP/CAIS Nº. 03/2025 (RETIFICAÇÃO EDITAL RNP/CAIS Nº. 02/2025)

RETIFICAÇÃO EDITAL RNP/CAIS Nº. 02/2025		
ITENS RETIFICADOS	**4.11.**	Inclusão da definição sobre arranjos locais;
	7.1.	Ajuste na elegibilidade das proponentes para submissão da proposta;
	8.1.	Inclusão do incentivo à formação dos arranjos locais;
	8.3.	Inclusão das licenças fornecidas; Ajuste na quantidade de certificações fornecidas;
	8.4.	Inclusão do processo de definição das instituições atendidas;
	9.3.	Ajuste na parte contratual e número de analistas;
	9.4.	Nova cláusula sobre o horário de funcionamento do SOC Distribuído;
	10.1.4.	Expansão do prazo para submissão de candidaturas;
	11.1.	Expansão do prazo para publicação do resultado;
	12.3.	Remoção do critério avaliado “Equipe”; Ajuste na pontuação do critério avaliado “Arranjos locais: equipe”;
	14.1.3.	Ajuste no número de analistas;

1ª Seleção de Instituições para o Estabelecimento de Centros de Operações de Segurança (SOC) Distribuídos Integrados à Rede Federada de Cibersegurança

26 de abril de 2025

A REDE NACIONAL DE ENSINO E PESQUISA, associação civil qualificada como Organização Social pelo Decreto nº 4.077 de 09 de janeiro de 2002, com sede à Rua Lauro Müller nº 116, sala 1103, Botafogo, Rio de Janeiro, RJ, CEP 22290-160, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob o nº 03.508.097/0001-36, por meio deste Edital, selecionará 2 (dois) proponentes para firmar um Acordo de Cooperação Técnica (ACT) com o objetivo de estabelecer 1 (um) Centro de Operações de Segurança (SOC) Distribuído cada, e por consequência participação na chamada Rede Federada de Cibersegurança.

1. CONTEXTUALIZAÇÃO

1.1. A RNP é a rede acadêmica brasileira para educação e pesquisa, com objetivo geral de promover o uso inovador de redes avançadas no Brasil. Ela disponibiliza internet segura e de alta capacidade, serviços personalizados e promove projetos de inovação. Colabora com redes nacionais de educação e pesquisa de outros países, conhecidas como *National Research and Education Networks* (NRENs). A RNP foi criada em 1989, contribuiu para a chegada da Internet no Brasil, e hoje a Rede Ipê, seu backbone nacional, serve às instituições de todas as unidades da federação. A RNP está conectada às demais redes de educação e pesquisa na América Latina, América do Norte, África, Europa, Ásia e Oceania por meio de cabos de fibra óptica terrestres e submarinos. Com a Rede Ipê, seu backbone nacional de alta capacidade, mais de 1.800 campi são conectados, em centenas de localidades em todo o Brasil, incluindo universidades, centros de pesquisa, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos. Somado ao desenvolvimento, sustentação e oferta de serviços e aplicações de TIC, beneficia cerca de 4,5 milhões de alunos, professores e pesquisadores brasileiros. Implementa soluções de TIC próprias, construídas por meio de processos de desenvolvimento tecnológico envolvendo grupos e instituições de pesquisa brasileiros e setor privado.

1.2. O pioneirismo também existe em cibersegurança. Em 1995 a RNP criou o primeiro centro de segurança de redes brasileiro, que deu origem ao CAIS[1] em 1997, cujo papel é zelar pela segurança da rede e das instituições conectadas. Com mais de 28 anos de atuação, o CAIS foi um dos primeiros grupos de resposta a incidentes de segurança a atuar em nível nacional na detecção, resolução e prevenção de incidentes de segurança cibernética. Atualmente, o CAIS trata da segurança da informação de uma forma holística, com ações integradas e colaborativas de governança, identificação, proteção, detecção, resposta e recuperação. O CAIS possui um papel relevante[2] para a comunidade, com a publicação de estatísticas, alertas, notificações[3] e relatórios de segurança[4], e mantém um Catálogo de Fraudes[5]. Para o cumprimento dos objetivos estratégicos, a segurança da informação e a privacidade sempre foram e continuam sendo fundamentais para a RNP.

[1] 25 anos do CAIS. http://plataforma.rnp.br/cais/25-anos
[2] CAIS, inteligência em cibersegurança. https://www.rnp.br/cais/
[3] Estatísticas do CAIS. https://www.rnp.br/cais/#Estatisticas
[4] Pesquisas, relatórios e conteúdos ricos em informação. https://www.rnp.br/informe-se/publicacoes/
[5] Catálogo de Fraudes. https://catalogodefraudes.rnp.br

1.3. O Brasil possui a Estratégia Nacional de Segurança Cibernética (e-ciber)[6], que direciona ações estratégicas que reforçam o papel de estados e municípios para a proteção e resiliência cibernética da sociedade, pessoas e instituições.

1.4. Os números de incidentes cibernéticos seguem aumentando, resultando em prejuízos para pessoas e instituições[7].

1.5. A cibersegurança é um pilar fundamental para alavancar o desenvolvimento econômico[8], principalmente devido ao aumento da conectividade e da digitalização, que resulta em uma maior superfície de ataques cibernéticos.

1.6. A privacidade e segurança é um dos objetivos da Estratégia Nacional de Governo Digital[9], visando ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

1.7. O Programa de Privacidade e Segurança da Informação (PPSI)[10], tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

1.8. Alinhado ao PPSI e às necessidades correlatas em Segurança da Informação, a RNP inaugurou em 2023 o SOC-RNP, implantado para proporcionar maior proteção, visibilidade, mitigação de ataques cibernéticos e conformidade para as instituições que fazem parte do Sistema RNP. O modelo de custos compartilhados viabiliza o atendimento às instituições (atualmente em mais de 90) por meio de parcerias, uso em escala de plataformas de cibersegurança e time especializado, que resultam em custos reduzidos se comparados aos de mercado.

1.9. Com a aderência às necessidades de cibersegurança das instituições, e diante dos desafios crescentes, derivou-se do SOC-RNP o conceito de torná-lo distribuído - SOCs Distribuídos. O objetivo é de desenvolver capacidades de cibersegurança próprias nos estados brasileiros,

[6] Decreto N. 10.222, de 5 de fevereiro de 2020. https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf
[7] Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros
[8] Cybersecurity Economics for Emerging Markets. https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets
[9] Estratégia Nacional de Governo Digital. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional
[10] Portaria SGD/MGI Nº 852, de 28 de março de 2023. https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908

de uma forma coordenada com o SOC-RNP, fortalecendo assim as instituições locais, que terão maior visibilidade, proteção e resiliência cibernética, avançando também no nível de maturidade e conformidade, em especial com a propagação de ações do PPSI.

1.10. Atuando de forma coletiva, integrada e coordenada, os SOCs Distribuídos atuarão com o SOC-RNP, que passa a exercer um papel central, como um SOC de Coordenação, trazendo toda a expertise e experiência exercida nos 28 anos de CAIS em cibersegurança.

1.11. Os SOCs Distribuídos representam os alicerces que sustentarão a construção de uma Rede Federada de Cibersegurança da RNP, representando uma estrutura colaborativa, descentralizada, expansiva e incremental de desenvolvimento de capacidades de cibersegurança.

1.12. Existe uma grande necessidade de fortalecimento dos estados brasileiros em segurança cibernética, que está alinhada com o propósito do SOC Distribuído. Com o desenvolvimento de capacidades em cibersegurança e a construção da Rede Federada de Cibersegurança, esta iniciativa contribui para a evolução da cultura em cibersegurança, do nível de maturidade, da conformidade e da capacidade de proteção contra os ataques cibernéticos e resposta avançada a incidentes de segurança.

2. FUNDAMENTAÇÃO

2.1. As necessidades de cibersegurança exigem uma atuação coletiva, com sinergias e ações em nível nacional, estadual e municipal. Adicionalmente, a atuação setorial reforça a assertividade das ações, permitindo a priorização, otimização e a escalabilidade. A RNP, por meio do CAIS, vem, ao longo dos anos, atuando com abrangência nacional na conectividade segura de todo o Brasil, tendo como parte essencial os Pontos de Presença (PoPs) distribuídos em todos os estados brasileiros.

2.2. O CAIS da RNP vem acompanhando as necessidades e evoluções de cibersegurança, com o desenvolvimento de capacidades relacionadas à gestão de segurança da informação, gestão de riscos cibernéticos e de vulnerabilidades, proteção e implementação de controles de segurança, monitoramento, resposta a incidentes e recuperação de desastres. O CAIS tem reforçado a atuação necessária no ecossistema de ensino, pesquisa e inovação com a estruturação de seu Centro de Operações de Segurança (SOC), trabalhando de forma integrada com as frentes complementares de segurança ofensiva (*Red Team*) e defensiva (*Blue Team*), governança, riscos, conformidade, privacidade, educação, conscientização, resposta a incidentes (CSIRT) e arquitetura de segurança.

2.3. O SOC-RNP vem contribuindo para a elevação do nível de cibersegurança das Organizações Usuárias do Sistema RNP, incluindo avanços relacionados aos controles do PPSI, aumento da resiliência cibernética, melhoria da visibilidade de cibersegurança, e redução de impactos financeiros e reputacionais decorrentes de ataques cibernéticos.

2.4. Diante do cenário atual, em que os impactos dos incidentes cibernéticos são cada vez mais representativos e as medidas legais exercidas pelos países continuam a evoluir, torna-se essencial o avanço das estratégias organizacionais e técnicas, que por sua vez exigem o desenvolvimento de capacidades e de medidas de cooperação.

2.5. A RNP busca estabelecer alianças estratégicas com os estados para fortalecer a cibersegurança com o estabelecimento de SOCs Distribuídos como elemento impulsionador para a proteção cibernética de instituições e pessoas, fundamentais para o desenvolvimento local, a partir do desenvolvimento de capacidades em cibersegurança.

2.6. Os SOCs Distribuídos atuarão de forma coletiva e integrada com o SOC RNP, que passará a exercer o papel de um SOC de Coordenação, contribuindo para os avanços locais.

2.7. A estruturação da RNP na forma de um sistema, o Sistema RNP, reformulado por meio da Portaria Interministerial n. 3.825, de 12 de dezembro de 2018, reflete uma proposta integradora, orientada pela articulação de iniciativas, recursos e capacidades em benefício das comunidades alcançadas e das organizações usuárias, integrantes do mencionado Sistema. Nesse mesmo sentido, portanto, no campo da cibersegurança, a RNP propõe uma atuação coletiva e coordenada, capaz de potencializar a proteção digital por meio de soluções compartilhadas e colaborativas, ampliando o alcance e a efetividade das ações de segurança.

2.8. Os SOCs Distribuídos, nesse sentido, constituem a primeira ação para a construção de uma Rede Federada de Cibersegurança, que visa implementar elementos da Estratégia Nacional de Cibersegurança (e-Ciber), agregando novas capacidades necessárias de segurança cibernética que refletirão em toda a sociedade, de uma forma sinérgica com as estratégias federais, estaduais e municipais. A Rede Federada de Cibersegurança visa instituir uma estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional, em especial o Programa de Privacidade e Segurança da Informação (PPSI) do governo federal.

3. BASE LEGAL

O presente edital encontra-se fundamentado nas seguintes normativas e dispositivos legais:

3.1. Decreto nº 4.077, de 09 de janeiro de 2002 – Qualificação da RNP como Organização Social.

3.2. Lei nº 12.846, de 1º de agosto de 2013 – Lei Anticorrupção, que define normas para integridade nas parcerias público-privadas.

3.3. Lei Complementar nº 101, de 4 de maio de 2000 – Lei de Responsabilidade Fiscal (LRF), que orienta o equilíbrio das contas públicas nas parcerias governamentais.

3.4. Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) – Estabelece princípios, direitos e deveres para o uso da Internet no Brasil, incluindo a proteção da segurança cibernética.

3.5. Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 – LGPD) – Regulamenta o tratamento de dados pessoais, essencial para a implementação do SOC.

3.6. Portaria Interministerial MEC/MCTIC nº 3.825, de 12.12.2018, que reformula o Programa Interministerial de Implantação e Manutenção da Rede Nacional para Ensino e Pesquisa - RNP e de seu Comitê Gestor.

4. DEFINIÇÕES

4.1. **Centro de Operações de Segurança da RNP (SOC-RNP**): O Centro de Operações de Segurança da RNP tem como objetivo fortalecer a segurança cibernética das Organizações Usuárias do Sistema RNP, elevando seu nível de maturidade e aprimorando a capacidade de detecção, prevenção e resposta a incidentes de segurança.

4.2. **Ciberinfraestrutura:** Plataforma digital distribuída, integrada por redes de comunicação, sistemas de computação e armazenamento, componentes de *hardware* e *software* e dispositivos de sensoriamento e aquisição de dados que, em conjunto, habilitam e suportam a pesquisa científica, a educação e a inovação.

4.3. **Entidade:** pessoa jurídica pública ou privada, dotada de personalidade jurídica própria.

4.4. **Instituição Abrigo:** Local físico em que o SOC Distribuído funcionará, com atuação do time, processos e plataformas tecnológicas de cibersegurança, integrado e em colaboração com o SOC de Coordenação.

4.5. **Organização Usuária:** Instituição pública ou privada habilitada para compartilhar da ciberinfraestrutura para Educação, Pesquisa e Inovação provida pela RNP e, por adesão, compor o Sistema RNP, usufruindo de seus serviços. As instituições que compartilham esta ciberinfraestrutura da RNP, são, portanto, “Organizações Usuárias do Sistema RNP”.

4.6. **Pontos de Presença (PoP):** Para operar seu backbone e garantir o atendimento às comunidades de educação, pesquisa, saúde e cultura, a RNP possui pontos de presença

(PoPs) espalhados pelas 27 unidades da federação. Nesses, equipes técnicas e administrativas são responsáveis por garantir acesso à rede Ipê para seus usuários finais, que podem estar vinculados a organizações que se conectam ao backbone diretamente, através dos PoPs, ou indiretamente, através de redes metropolitanas ou infovias estaduais ou regionais.

4.7. **Rede Federada de Cibersegurança:** Estrutura colaborativa, descentralizada, expansiva e incremental de desenvolvimento de capacidades de cibersegurança que, inicialmente, é composta pelas instituições responsáveis por abrigar o SOC Distribuído. Esse modelo fortalece a cultura de cibersegurança, contribui para a democratização da cibersegurança no Brasil, elevando a maturidade das operações e a capacidade de resposta avançada a incidentes de segurança.

4.8. **Sistema RNP[11]:** Sistema responsável pelo desenvolvimento, oferta e uso de serviços para atender às necessidades das comunidades de pesquisa, educação e inovação. Explora tecnologias de informação e comunicação emergentes, disponibilizando uma ciberinfraestrutura de recursos federados, seguros, de alta capacidade e desempenho, por meio de mecanismos de governança multi-institucional, estabelecidos pelo Programa Interministerial Rede Nacional de Ensino e Pesquisa – PRORNP, reformulado pela Portaria Interministerial nº 3.825, de 12 de dezembro de 2018. O Sistema RNP é composto por: (i) a Rede Nacional Ipê e seus Pontos de Presença (PoPs) e Pontos de Agregação; (ii) as Redes Metropolitanas Comunitárias; (iii) as Organizações Usuárias; e (iv) as Redes de Colaboração de Comunidades.

4.9. **SOC de Coordenação:** SOC-RNP, responsável por orquestrar os SOCs Distribuídos, garantindo as operações 24x7x365, as atualizações tecnológicas, o cumprimento dos processos, a qualidade nas entregas e uma atuação eficiente e rápida em casos de incidentes de segurança.

4.10. **SOC Distribuído:** Infraestrutura física e tecnológica local nos estados, com times de cibersegurança com a missão de proteger e monitorar ativamente as instituições locais contra ameaças cibernéticas. É orquestrado, organizado e integrado com o SOC de Coordenação, seguindo padrões e processos que garantem uma operação homogênea e eficiente. Parte fundamental para o desenvolvimento de capacidades de cibersegurança local e para a Rede Federativa de Cibersegurança.

4.11. **Arranjos Locais:** Articulações e parcerias institucionais voltadas a viabilizar a implementação, a operação e a sustentabilidade do SOC Distribuído. Essas colaborações podem envolver as

[11] https://www.rnp.br/sistema-rnp

10 (dez) instituições que venham a ser beneficiadas pelo SOC Distribuído, sem custo nos 2 (dois) primeiros anos do acordo, bem como outros órgãos ou entidades capazes de contribuir com recursos, infraestrutura ou profissionais qualificados. Os arranjos locais têm como principais objetivos estabelecer e manter a infraestrutura necessária ao funcionamento do SOC Distribuído, viabilizar a contratação e/ou alocação de equipe técnica, além de apoiar a expansão e o fortalecimento da Rede Federada de Cibersegurança. Considerando que este edital não prevê repasse financeiro por parte da RNP à instituição abrigo, tais parcerias são consideradas fundamentais para garantir a efetividade, a continuidade e o sucesso da iniciativa.

5. PROPÓSITO DO EDITAL DE SELEÇÃO PARA COOPERAÇÃO EM EXECUÇÃO DE POLÍTICA PÚBLICA

5.1. A finalidade deste Edital é a seleção de 2 (dois) proponentes, de diferentes Estados, para a celebração de parceria, por meio de Acordo de Cooperação Técnica (ACT), para desenvolver capacidades em cibersegurança e implantar SOC Distribuído no seu estado, visando proteger e monitorar instituições locais e iniciar a construção de uma Rede Federada de Cibersegurança.

5.2. Será selecionada uma única proposta por proponente, observada a ordem de classificação para a celebração do ACT.

6. OBJETIVO DO ACORDO DE COOPERAÇÃO TÉCNICA

6.1. O Acordo de Cooperação Técnica (ACT) que será celebrado após a realização da seleção tem como objetivo formalizar a cooperação com as instituições selecionadas para o fortalecimento das capacidades em cibersegurança, mediante a integração com o CAIS, a implantação de SOC Distribuído e a futura participação na Rede Federada de Cibersegurança em formação, promovendo, de forma conjunta entre os parceiros, ações coordenadas, escaláveis e sustentáveis voltadas à proteção e à resiliência cibernética de pessoas e instituições, em consonância com as diretrizes nacionais de segurança da informação e proteção de dados.

7. CRITÉRIOS DE ELEGIBILIDADE E CONDIÇÕES DE PARTICIPAÇÃO

7.1. São elegíveis para submissão de propostas as Organizações Usuárias do Sistema RNP, bem como outras instituições estaduais, tais como fundações, secretarias de governo, companhias estaduais de processamento de dados (PRODs) e entidades similares, público ou privado.

7.2. Arranjos locais são desejáveis e podem ser feitos para viabilizar a implantação do SOC Distribuído e integração à Rede Federada de Cibersegurança em formação.

7.3. Somente serão admitidas propostas que apresentem manifestação por escrito da alta gestão da instituição, assinada por dirigente com poderes legais para representação da instituição. O modelo de carta de anuência é apresentado no ANEXO I deste instrumento.

7.4. A participação das instituições interessadas neste Edital implica na aceitação de todas as condições aqui apresentadas.

8. RECURSOS E BENEFÍCIOS CONCEDIDOS

8.1. Não há previsão de repasse de recursos financeiros neste edital. No entanto, conforme descrito na Seção 12, são incentivados arranjos locais que promovam a cooperação entre instituições. Esses arranjos podem ter como objetivo o estabelecimento e a manutenção da infraestrutura necessária para a operação do SOC Distribuído, a viabilização da contratação e/ou alocação da equipe técnica, bem como o apoio à expansão da Rede Federada de Cibersegurança.

8.2. O proponente terá um Centro de Operações de Segurança (SOC) para o atendimento às instituições do estado, com alinhamento direto com as necessidades locais, com a Estratégia Nacional de Segurança Cibernética (e-ciber), visando o desenvolvimento de capacidades em cibersegurança necessários para evoluir a resiliência cibernética na região.

8.3. Para a execução da parceria decorrente desta seleção, serão fornecidos aos proponentes selecionados:

- Licenciamento e acesso as plataformas de cibersegurança designadas para a proposta do SOC Distribuído. Atualmente, as seguintes camadas de proteção são contempladas:
  - Anti-DDoS;
  - WAAP (WAF);
  - Gestão de Vulnerabilidades;
  - Threat Intelligence;
  - Security Ratings;
  - SIEM;
- Processos utilizados no SOC de Coordenação que possibilitam o funcionamento da operação de segurança a ser conduzida;
- Manuais de operação das plataformas de cibersegurança fornecidas pelo SOC de Coordenação;

- Treinamento interno da equipe que irá compor o SOC Distribuído;
- Certificações do curso Security+ da CompTIA para os 2 (dois) analistas selecionados para as atividades do SOC Distribuído;
- Arte da marca a ser utilizada pelo SOC Distribuído, contendo logomarcas da RNP, CAIS, SOC-RNP, instituição abrigo e participantes do arranjo local.

8.4. Será disponibilizado o licenciamento das plataformas de cibersegurança equivalente à atuação do SOC Distribuído, em conjunto com o SOC de Coordenação, em atividades de cibersegurança para 10 (dez) instituições do estado, durante 2 (dois) anos. O processo de definição das instituições do estado que serão atendidas será realizado em conjunto com a gestão do SOC Distribuído e SOC de Coordenação, priorizando o atendimento às instituições participantes do Sistema RNP.

8.5. Uma vez constituído o SOC Distribuído, o proponente e a RNP deverão construir e implantar, em conjunto, um modelo de atuação que sustente a expansão dos serviços para um número maior de instituições locais, além de viabilizar economicamente e financeiramente a continuidade das operações após os 2 (dois) anos.

8.6. Será oferecido, sem custo para a instituição abrigo selecionada, o serviço do SOC, que contemplará as seguintes camadas de segurança:

- Monitoramento e mitigação de ataques de negação de serviço;
- E-mail de Indicadores semanais;
- Gestão de vulnerabilidades (externas);
- Visibilidade de ataques cibernéticos, vulnerabilidades, ameaças e ataques;
- Classificação de riscos cibernéticos;
- Evolução histórica dos riscos cibernéticos;
- Relatório mensal com análise;
- Notificação / interação;
- Reunião mensal;
- Monitoramento e mitigação de ataques na camada de aplicação;

8.7. O SOC de Coordenação irá fornecer apoio operacional durante o período de operação do SOC Distribuído, garantindo uma redundância da operação de segurança.

8.8. Fora do horário de operação do SOC Distribuído, as atividades de segurança serão gerenciadas pelo SOC de Coordenação, assegurando cobertura ininterrupta.

8.9. Poderá ser fornecido ainda, capacitações e cursos para a equipe do SOC Distribuído, sem custo para a instituição abrigo, caso haja necessidade identificada pelo SOC de Coordenação.

9. DEVERES E RESPONSABILIDADES

INSTITUIÇÃO ABRIGO

A instituição abrigo deve atender aos seguintes itens, de acordo com o ACT que será estabelecido.

9.1. A instituição abrigo é responsável por prover a infraestrutura necessária para a implantação do SOC Distribuído, seguindo os seguintes padrões:

9.1.1. Infraestrutura física destinada exclusivamente para comportar a sala do SOC na instituição abrigo, onde, por questões de segurança, a sala não pode ser compartilhada com nenhuma outra equipe que não a do SOC Distribuído. Essa infraestrutura deve possuir os seguintes itens:

- Metragem mínima de 25 m²;
- Parede adesivada com a arte da marca a ser utilizada pelo SOC Distribuído, contendo logomarcas da RNP, CAIS, SOC-RNP, instituição abrigo e participantes do arranjo local;
- Ar-condicionado;
- Mesas, Cadeiras e Gaveteiros;
- Fechadura com leitor biométrico;
- Porta com fechamento magnético;
- Câmera de vigilância;
- Vidro Polarizado;
- Link cabeado para todas as estações de trabalho;
- Telefone e sistema de mensageria;
- Questões relacionadas à eletricidade, sobretudo sobre disponibilidade de energia elétrica, de preferência, ininterrupta (geradores e nobreaks), inclusive para ou com capacidade de manter o sistema de refrigeração para conforto dos alocados e equipamentos.

9.1.2. O ambiente escolhido para a implantação do SOC Distribuído, incluindo o *layout* de todos os itens definidos acima, deve ser aprovado mediante visita técnica presencial

da equipe do SOC de Coordenação da RNP, a fim de garantir uma estrutura adequada e padronizada para comportar de maneira profissional a operação do SOC Distribuído.

9.1.3. Os requisitos mínimos do conjunto de equipamentos de TIC destinados à equipe que irá compor o SOC Distribuído e ao ambiente físico são:

- Equipamentos para Vídeo Wall:
  - 4 (quatro) TVs de 50 a 55 polegadas;
  - 1 (um) computador com processador i7, placa de vídeo com 4 (quatro) saídas HDMI, SSD 500GB, 32GB de memória RAM; **ou** 2 (dois) computadores com processador i5, placa de vídeo com 2 (duas) saídas HDMI, SSD 500GB, 16GB de memória RAM.
- Equipamento individual da equipe:
  - 1 (um) notebook com processador i5, SSD 500GB, 16GB de memória RAM e *webcam* integrada;
  - 2 (dois) monitores de tamanho entre 21 e 23 polegadas;
  - 1 (um) *dock station* com duas entradas *display port* ou HDMI, e conexão USB-A;
  - 1 (um) kit teclado e mouse sem fio;
  - 1 (um) fone headset com microfone.

9.1.4. Conectividade geral:

- Conexão ethernet cabeada para todas as estações de trabalho;
- Cabeamento necessário para a interconexão dos equipamentos;
- Uso de VPN;
- Redundância de links.

9.1.5. Outros equipamentos poderão ser instalados caso a RNP verifique a necessidade e a instituição abrigo concorde, para cumprimento dos objetivos do projeto. Neste caso, a instituição será previamente informada da possível demanda adicional.

9.2. A instituição abrigo deve custear todas as despesas operacionais (como água, energia elétrica, entre outros), além de garantir a manutenção e, se necessário, a substituição dos recursos essenciais para o pleno funcionamento do SOC Distribuído.

9.3. A instituição abrigo é responsável pela contratação e/ou alocação de, no mínimo, 2 (dois) analistas de segurança minimamente qualificados para atuar simultaneamente, de forma

presencial e exclusiva no SOC Distribuído, não sendo permitido o trabalho em regime remoto ou híbrido (remoto e presencial). É permitido que o analista possua qualquer tipo de vínculo contratual com a instituição, desde que a exclusividade seja garantida de forma que não haja sobreposição de atribuições durante o horário de sua atuação no SOC Distribuído. Por exemplo, em caso de bolsistas, atividades vinculadas a outro projeto de pesquisa não devem ser realizadas durante o período destinado à atuação no SOC Distribuído.

9.4. O SOC Distribuído deverá operar em regime de expediente regular, com funcionamento de segunda a sexta-feira, das 9h às 18h, respeitando os feriados locais e nacionais. A instituição abrigo deve assegurar a presença dos analistas alocados durante todo o período de funcionamento, conforme as exigências de dedicação e exclusividade descritas anteriormente.

9.5. A equipe do SOC Distribuído não poderá operar nenhuma plataforma interna da instituição abrigo, que já não faça parte do escopo de monitoramento delimitado pelo SOC de Coordenação.

9.6. A substituição ou reposição dos analistas deve ocorrer no menor prazo possível, de forma a evitar descontinuidade nas atividades do SOC Distribuído. O não cumprimento dessa obrigação poderá resultar em notificação formal pela equipe do SOC de Coordenação da RNP, concedendo um prazo para regularização da equipe.

9.7. A instituição abrigo deve contratar e/ou alocar um responsável técnico, podendo ser o gestor de TIC ou o gestor de cibersegurança, a fim de gerir a equipe de analistas do SOC Distribuído.

9.8. O responsável técnico do SOC Distribuído é o ponto central de contato para todas as questões gerenciais, atuando em conjunto com o responsável técnico do SOC de Coordenação.

9.9. Em caso de ausência do responsável técnico, a instituição abrigo deve indicar um substituto qualificado que assumirá temporariamente as responsabilidades dele, garantindo a continuidade das operações do SOC Distribuído;

9.10. Caso a ausência do responsável técnico seja prolongada ou definitiva, a instituição abrigo deve nomear um novo profissional no menor prazo possível, assegurando que o SOC Distribuído não sofra prejuízos operacionais.

9.11. Em caso de ausência, de qualquer natureza, o responsável técnico da instituição deve comunicar o SOC de Coordenação via e-mail, com a maior brevidade possível.

9.12. A instituição abrigo deve fornecer informações sobre horários de funcionamento, recessos e feriados com, no mínimo, 48 horas de antecedência. Este informe deve ser enviado ao time de coordenação do SOC da RNP, via e-mail soc@rnp.br.

9.13. O SOC Distribuído deve cumprir integralmente os processos e procedimentos definidos pelo SOC de Coordenação, garantindo o mesmo nível de qualidade. Além disso, deve viabilizar a validação e análise contínua pelo SOC de Coordenação, assegurando a consistência na execução dos processos e a eficiência operacional.

9.14. O SOC Distribuído deve manter o padrão de qualidade estabelecido pelo SOC de Coordenação.

9.15. O SOC Distribuído deve possibilitar a validação e análise dos padrões de qualidade e do cumprimento dos processos e procedimentos estabelecidos.

9.16. O SOC Distribuído deve passar anualmente por checagem de conformidade dos padrões de qualidade e maturidade nos processos e procedimentos provenientes da padronização do SOC de Coordenação. É necessário envio de documentações e evidências aderentes aos padrões pré-determinados.

9.17. O proponente e a RNP devem construir e implantar, em conjunto, um modelo de atuação que sustente a expansão dos serviços para um número maior de instituições locais, além de viabilizar economicamente e financeiramente a continuidade das operações após 2 (dois) anos, considerando a Rede Federada em Cibersegurança, potenciais arranjos locais e políticas públicas em cibersegurança.

9.18. Não está prevista a transferência de recursos financeiros para as instituições abrigo selecionadas. Quaisquer despesas relacionadas à ampliação da infraestrutura física ou à aquisição de equipamentos necessários é de responsabilidade integral da instituição abrigo.

RNP

9.19. A RNP deve custear o licenciamento das soluções utilizadas no SOC de Coordenação, que serão fornecidas ao SOC Distribuído.

9.20. O SOC de Coordenação deve orquestrar toda a operação de segurança, fornecendo capacidade e inteligência em cibersegurança por meio das soluções, processos e manuais fornecidos.

9.21. O SOC de Coordenação é responsável por manter a operação de segurança 24x7, visto que o SOC Distribuído atua apenas em horário comercial. O SOC Distribuído deve realizar a troca

de conhecimento com o SOC de Coordenação durante a troca de horário, a fim de manter a operação de segurança durante a madrugada, feriados e fins de semana.

9.22. O SOC de Coordenação é responsável por orquestrar e direcionar as atividades da equipe do SOC Distribuído, seja para tratar de questões relacionadas à própria instituição abrigo ou às demais instituições monitoradas pelo SOC.

9.23. O SOC de Coordenação deve apoiar o processo de seleção dos analistas e responsável técnico que irão compor a equipe do SOC Distribuído.

9.24. A equipe técnica do SOC de Coordenação da RNP deve avaliar a equipe do SOC Distribuído, a fim de garantir a qualidade nas atividades, incluindo as respostas a incidentes de segurança.

9.25. O SOC de Coordenação deve avaliar periodicamente o padrão de qualidade e a efetividade do SOC Distribuído (conformidade com os processos e procedimentos estabelecidos no SOC de Coordenação), incluindo uma análise do nível de maturidade, a partir de suas entregas.

9.26. A RNP poderá convidar, a seu critério e arcando com os custos de locomoção, estadia e alimentação, a participação de membros da equipe do SOC Distribuído em reuniões de trabalho, ações de capacitação ou em eventos organizados pela RNP.

9.27. O proponente e a RNP devem construir e implantar, em conjunto, um modelo de atuação que sustente a expansão dos serviços para um número maior de instituições locais, além de viabilizar economicamente e financeiramente a continuidade das operações após 2 (dois) anos, considerando a Rede Federada em Cibersegurança, potenciais arranjos locais e políticas públicas em cibersegurança.

10. APRESENTAÇÃO DA PROPOSTA E DA DOCUMENTAÇÃO

10.1. Apresentação da proposta:

10.1.1. A apresentação de candidaturas deverá ser realizada por meio do preenchimento e envio, por parte do proponente, do formulário eletrônico disponível no endereço: https://forms.office.com/r/0BUBq4rHqR

10.1.2. A pessoa a ser identificada como proponente no formulário de submissão precisa pertencer ao quadro de funcionários da instituição, bem como deverá ser utilizado, necessariamente, seu endereço de e-mail institucional para envio da proposta.

- Recomenda-se que o proponente seja o gestor de segurança da informação ou de TI da instituição.

10.1.3. Além do preenchimento do formulário eletrônico, cada proponente deverá apresentar uma manifestação favorável, em apoio à proposta, da alta gestão da instituição (dirigente com poderes legais para representação da instituição).

- Tal manifestação poderá ser comprovada por meio de ofício ou mensagem eletrônica enviada para o endereço soc@rnp.br.

10.1.4. Serão consideradas as propostas enviadas até às 23:59 do dia 16/05/2025, no fuso horário GMT-3.

- Este mesmo prazo também é aplicável para as manifestações de anuência do dirigente e do gestor de segurança da informação/TI da instituição.

10.1.5. Após o término do prazo estabelecido, nenhuma outra proposta será recebida, assim como não serão aceitos adendos ou esclarecimentos que não forem solicitados pela RNP.

10.2. Envio de informações complementares:

10.2.1. A RNP se compromete a tratar de forma confidencial toda informação e documentação que venha a ter acesso por força desde edital, obrigando-se a utilizá-las apenas para a finalidade e nos limites aqui apresentados e a não permitir que nenhum de seus colaboradores, representantes ou terceiros sob sua responsabilidade, façam quaisquer outros usos dessas informações confidenciais sem prévia autorização do proponente.

10.2.2. A Comissão de Seleção poderá entrar em contato com o proponente a qualquer tempo, se julgar necessário, para o esclarecimento de dúvidas técnicas que possam surgir durante a análise da proposta enviada.

11. PRAZOS

11.1. Prazos do cronograma deste Edital:

FASE	DATA
Publicação deste Edital	21/03/2025
Retificação	26/04/2025
Webconferência pública para tirar dúvidas sobre este Edital, a ser realizada no endereço: **https://conferenciaweb.rnp.br/sala/soc-rnp**	04/04/2025 às 14h (GMT -3)

Término do prazo para submissão de candidaturas.	16/05/2025
Publicação do resultado.	Até 20/06/2025
Assinatura do Acordo de Cooperação Técnica (ACT).	Em até 30 dias após a publicação do resultado

11.2. O horário limite para a submissão das propostas e entrega de documentação se encerra às 23:59 (fuso horário GMT-3).

11.3. O prazo limite para a adequação integral da infraestrutura do SOC Distribuído (seções 9.1, 9.3 e 9.6) é de até 3 (três) meses após a assinatura do ACT.

11.4. Após a publicação do resultado, a RNP entrará em contato com os proponentes selecionados para o agendamento de uma reunião inaugural (*kick-off*).

12. CLASSIFICAÇÃO DAS PROPOSTAS

12.1. A Comissão de Seleção analisará as propostas apresentadas pelas instituições que aplicarem para este edital. A análise e a seleção das propostas serão realizadas pela Comissão de Seleção, que terá total independência técnica para exercer seu julgamento.

12.2. A Comissão de Seleção será composta por analistas e gestores da RNP, incluindo aqueles que atualmente compõem o SOC de Coordenação da RNP, e representante do MCTI.

12.3. A classificação dos proponentes será realizada por meio da avaliação dos seguintes critérios:

Critério avaliado	**Aspectos que serão considerados na avaliação**	**Pontuação atribuída**
Instituição abriga um Ponto de Presença (POP) da RNP	Atualmente hospeda um Ponto de Presença (PoP) da RNP em sua infraestrutura.	0 ou 1 Peso 5
Instituição abriga uma unidade da Escola Superior de Redes (ESR)	Atualmente hospeda uma unidade da Escola Superior de Redes (ESR) em sua infraestrutura.	0 ou 1 Peso 3
Conectividade ao Sistema RNP	Pontuação de acordo com a capacidade do link ao Sistema RNP. Quanto maior a conectividade, maior a pontuação.	1 Gb/s - 2 5 Gb/s - 3 10 Gb/s - 4 Peso 1

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
Conectividade redundante	Possui redundância dos links de Internet.	0 ou 1 Peso 3
Instituição oferta cursos de segurança da informação	Oferta cursos de segurança da informação em sua grade curricular, promovendo a capacitação e o aprimoramento contínuo das equipes que podem integrar o SOC.	0 ou 1 Peso 3
Infraestrutura	A proponente já possui toda a infraestrutura necessária para implantação do SOC Distribuído, de acordo com os itens descritos na seção 9.1.	0 ou 1 Peso 5
Experiência em cibersegurança do responsável técnico	Pontuação de acordo com a experiência, em anos.	Até 2 anos – 2 2-4 anos – 3 Acima de 4 anos - 4
Experiência em cibersegurança da equipe de analistas	Pontuação de acordo com a experiência, em anos, em média.	0-1 ano – 2 1-2 anos – 3 Acima de 2 anos - 4
Possui acordo de cooperação com o CAIS	Possui acordos de cooperação vigentes com a RNP ou o CAIS.	0 ou 1 Peso 1
Arranjos locais: equipe	A proponente possui uma equipe já estabelecida, que será alocada exclusivamente para atuação no SOC Distribuído (seções 9.3 e 9.6).	0 a 3 Peso 4
	A proponente dispõe de recursos financeiros próprios ou provenientes de cooperação e/ou acordos financeiros que assegurem o financiamento necessário para a manutenção da	0 ou 1 Peso 5

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
	equipe responsável pela continuidade do SOC Distribuído (seção 9.3 e 9.6 deste documento), a exemplo de financiamento do governo estadual.	
Arranjos locais: instituições	Possui relacionamentos institucionais com instituições que receberão os serviços. São aceitos para comprovação do item, documentos oficiais, como por exemplo, acordos institucionais, contratos, memorandos etc.	0 ou 1 Peso 3
Arranjos locais: expansão	Possui relacionamentos institucionais que viabilizem a expansão da Rede Federada de Cibersegurança. São aceitos para comprovação do item, documentos oficiais, como por exemplo, acordos institucionais, contratos, memorandos etc.	0 ou 1 Peso 4
Diversidade de estados atendidos	Receberão pontuação adicional proponentes dos seguintes estados: • AC - Acre • AL - Alagoas • AM - Amazonas • AP - Amapá • BA - Bahia • CE - Ceará • ES - Espírito Santo • GO - Goiás • MA - Maranhão • MG - Minas Gerais • MS - Mato Grosso do Sul • MT - Mato Grosso • PA - Pará • PB - Paraíba • PE - Pernambuco • PI - Piauí • PR - Paraná	0 ou 1 Peso 1

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
	• RJ - Rio de Janeiro • RN - Rio Grande do Norte • RS - Rio Grande do Sul • RO - Rondônia • RR - Roraima • SC - Santa Catarina • SE - Sergipe • TO - Tocantins	

12.4. A Comissão de Seleção apresentará como resultado duas listas ranqueadas das propostas: um ranqueamento geral e um ranqueamento por estado.

12.5. Havendo empate na classificação das propostas, serão adotados como critérios para desempate: “impacto para a cibersegurança do Brasil e para a sociedade” e “de acordo com as estratégias da RNP e do CAIS”, respectivamente.

12.6. Após recebimento das propostas, será realizada uma **etapa eliminatória,** onde os seguintes itens serão avaliados:

i. Recebimento de carta de anuência do Gestor de segurança da informação/TI (caso ele não seja o proponente).

ii. Organizações que possuem conectividade inferior a 1 Gb/s estão automaticamente desclassificadas.

iii. Instituições que não possuem infraestrutura física previamente destinada para comportar o SOC Distribuído estão automaticamente desclassificadas.

iv. De acordo com o ranqueamento das proponentes baseado na pontuação previamente estabelecida na seção 12.3, será feita uma visita técnica no local proposto para instalação do SOC Distribuído, a fim de avaliar a viabilidade técnica da implantação do mesmo. Caso seja avaliado que a instituição não está de acordo com os itens presentes neste documento, estará automaticamente desclassificada.

12.7. A Comissão de Seleção poderá realizar visitas às instituições com maior pontuação, a fim de emitir um parecer técnico sobre as instalações que irão receber o SOC Distribuído. Como resultado, será elaborado um parecer de caráter eliminatório, declarando a organização usuária apta ou inapta a abrigar o SOC Distribuído.

12.8. O proponente que impossibilitar e/ou não disponibilizar agenda dentro do prazo previsto para a visita técnica será automaticamente desclassificada.

13. RESULTADO

13.1. Os 2 (dois) proponentes mais bem classificados e que tenham cumprido com êxito a fase de análise da documentação serão declarados aptos para a celebração do ACT, sendo o resultado do edital homologado e publicizado.

13.2. Não será admitido mais de um proponente selecionado por estado.

13.3. O resultado será publicizado por meio do envio aos endereços eletrônicos informados pelos proponentes participantes e da divulgação da lista com as instituições aprovadas em página do website público da RNP (www.rnp.br).

14. RESCISÃO DO ACT

14.1. O Acordo de Cooperação Técnica (ACT) poderá ser rescindido caso o proponente deixe de atender aos requisitos técnicos e operacionais previamente estabelecidos, incluindo, mas não se limitando a:

14.1.1. Falha na manutenção da infraestrutura necessária para a operação do SOC distribuído, incluindo conectividade mínima;

14.1.2. Não substituição ou alocação de equipamentos essenciais à operação do SOC, comprometendo sua funcionalidade;

14.1.3. Caso a instituição abrigo não mantenha no mínimo 02 (dois) analistas atuando simultaneamente, de forma presencial e exclusiva para o SOC Distribuído;

14.1.4. Descumprimento de exigências regulatórias e normativas, não se limitando a:

i. Atender às exigências da Lei Geral de Proteção Dados (LGPD - Lei n. 13.709/2018), garantindo boas práticas no tratamento de dados pessoais;

ii. Cumprir o Marco Civil da Internet (Lei n. 12.965/2014), respeitando os princípios de privacidade, segurança e governança da informação;

iii. Seguir as diretrizes de segurança da RNP e do SOC de Coordenação, aderindo a padrões de operação e boas práticas recomendadas;

iv. Atender aos critérios do Plano de Trabalho, que estabelecerá as etapas, atividades e metas para a implantação do SOC Distribuído no estado.

15. DÚVIDAS E CONSULTAS

15.1. As consultas e os pedidos de esclarecimento referentes a este Edital deverão ser encaminhados à Comissão de Seleção, via Internet, para o e-mail **soc@rnp.br**, até a data da publicação do resultado.

15.2. A Comissão de Seleção terá prazo de 3 (três) dias úteis para responder as consultas e os pedidos de esclarecimentos encaminhados. As respostas serão enviadas para o e-mail do solicitante.

15.3. A RNP não se responsabiliza por quaisquer incorreções e/ou problemas de funcionamento dos endereços eletrônicos fornecidos pelas instituições interessadas.

16. DISPOSIÇÕES GERAIS

16.1. Será facultado à Comissão de Seleção promover, em qualquer fase do processo de análise e seleção, diligências destinadas a esclarecer ou complementar a instrução do presente Edital e a aferição dos critérios de habilitação de cada instituição.

16.2. A RNP poderá revogar o presente edital, no todo ou em parte, por conveniência e interesse público, ou por fato superveniente, devidamente justificado, ou anulá-lo, em caso de ilegalidade.

16.3. A revogação ou anulação do presente chamamento não gera direito a indenizações de quaisquer naturezas.

16.4. A divulgação do resultado da seleção da instituição não implica relação de obrigatoriedade para a formalização da parceria, contudo, havendo a celebração do ACT, ele terá efeito vinculante.

16.5. Todos os custos decorrentes da elaboração das propostas e quaisquer outras despesas correlatas à participação neste edital serão de inteira responsabilidade das instituições, não cabendo nenhuma remuneração, apoio ou indenização por parte da RNP.

16.6. O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da seleção.

16.7. No período entre a divulgação do resultado e a assinatura do ACT, o proponente fica obrigado a informar qualquer evento superveniente que possa prejudicar a celebração da parceria, sobretudo quanto ao cumprimento dos requisitos e exigências previstos para celebração do ACT.

16.8. As questões não previstas neste Edital serão decididas pela Comissão de Seleção e pela Diretoria Executiva da RNP, observadas as disposições legais aplicáveis.

17. DO FORO

17.1. Fica o foro do Rio de Janeiro, com renúncia a qualquer outro, por mais privilegiado que seja eleito para dirimir as dúvidas e questões oriundas do presente Edital que não possam ser resolvidas administrativamente.

ANEXO I

MODELO SUGESTIVO DE CARTA DE ANUÊNCIA

Eu, <nome>, <cargo>, na condição de dirigente do(a) <nome da instituição>, manifesto meu apoio à proposta submetida por <nome do proponente>, <cargo do proponente> desta instituição, em atendimento ao Edital de Seleção para Cooperação em Execução de Política Pública voltada ao estabelecimento de Centros de Operações de Segurança (SOC) Distribuídos integrados à Rede Federada de Cibersegurança.

Caso nossa proposta seja uma das selecionadas, estou ciente que será solicitado a assinatura de um Acordo de Cooperação Técnica em até 30 dias após a divulgação do resultado.